CLAIMS

What is claimed is:

1. A machine-implemented method for managing access to data, the method comprising the steps of:

detecting that a database command is issued;

wherein said database command requires access to at least one column in a table;

rewriting said database command by creating a modified database command, based on the database command;

wherein the modified database command specifies whether to mask a value of at least one column by returning a mask of the value instead of the value; and

executing said modified database command.

2. The method of claim 1,

wherein said database command requests at least two values located in at least two columns;

wherein each of the two values are located in a different one of the at least two columns; and

wherein the step of executing the modified database command includes at least returning at least one of the at least two values, and

returning a masked value instead of at least a second of the at least two values.

3. The method of claim 1, wherein the modified database command

includes at least

a condition expression returned by a policy function.

4. The method of claim 1, wherein the masked value is returned for rows that are retrieved for the database command issued, do not satisfy the condition, and to which access privileges are granted.

5. The method of claim 1, further comprising:

storing metadata that associates a list of one or more columns with a policy used for controlling access to the one or more columns;

wherein the step of rewriting is performed if a match is found between the at least one column to which the database command requires access and the list of one or more columns.

6. The method of claim 1, further comprising:

storing metadata that associates a list of one or more columns with a policy used for controlling access to the one or more columns;

wherein the step of creating is not performed if a match is not found between the list of one or more columns and the at least one column to which the database command requires access.

7. The method of claim 1, further comprising:

creating a policy function that returns a condition expression;

wherein the step of creating the modified database command includes incorporating the condition expression and the database command into the modified database command.

8. The method of claim 7, further comprising:

creating a policy referencing the policy function and specifying trigger columns that trigger implementing the policy.

9. The method of claim 1, further comprising registering a policy function with a database server, wherein the policy function returns a condition expression and the modified database command is based on the condition expression.

10. A machine-implemented method for managing access to data, the method comprising the steps of:

detecting that a database command is issued;

detecting that said database command requires access to at least one column in a table;

in response to detecting that the database command requires access to the at least one column, creating a modified database command by selectively adding zero or more predicates that are satisfied by rows in said table to which said user is permitted access.

11. A machine-readable medium carrying one or more sequences of instructions, which when executed by one or more processors, causes the one or more processors to perform a method comprising the steps of:

detecting that a database command is issued;

wherein said database command requires access to at least one column in a table;

rewriting said database command by creating a modified database command, based on the database command;

wherein the modified database command specifies whether to mask a value of at least one column by returning a mask of the value instead of the value; and

executing said modified database command.

12. The machine readable medium of claim 1,

wherein said database command requests at least two values located in at least two columns;

wherein each of the two values are located in a different one of the at least two columns; and

wherein the step of executing the modified database command includes at least returning at least one of the at least two values, and

returning a masked value instead of at least a second of the at least two values.

13. The machine-readable medium of claim 1, wherein the modified database command includes at least a condition expression returned by a policy function.

14. The machine-readable medium of claim 1, wherein the masked value is returned for rows that are retrieved for the database command issued,

do not satisfy the condition, and

to which access privileges are granted.

15. The machine-readable medium of claim 1, wherein the method further comprises:

storing metadata that associates a list of one or more columns with a policy used for controlling access to the one or more columns;

wherein the step of rewriting is performed if a match is found between the at least one column to which the database command requires access and the list of one or more columns.

16. The machine-readable medium of claim 1, wherein the method further comprises:

storing metadata that associates a list of one or more columns with a policy used for controlling access to the one or more columns;

wherein the step of creating is not performed if a match is not found between the list of one or more columns and the at least one column to which the database command requires access.

17. The machine-readable medium of claim 1, wherein the method further comprises:

creating a policy function that returns a condition expression;

wherein the step of creating the modified database command includes incorporating the condition expression and the database command into the modified database command.

18. The machine-readable medium of claim 7, wherein the method further comprises:

creating a policy referencing the policy function and specifying trigger columns that trigger implementing the policy.

19. The machine-readable medium of claim 1, wherein the method further comprises registering a policy function with a database server, wherein the policy function returns a condition expression and the modified database command is based on the condition expression.

20. A machine-readable medium carrying one or more sequences of instructions, which when executed by one or more processors, causes the one or more processors to perform a method comprising the steps of:

detecting that a database command is issued;

detecting that said database command requires access to at least one column in a table;

in response to detecting that the database command requires access to the at least one column, creating a modified database command by selectively adding zero or more predicates that are satisfied by rows in said table to which said user is permitted access.